UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

UNITED STATES, *et al.*,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

No. 1:23-cv-00108-LMB-JFA

GOOGLE LLC'S MEMORANDUM OF LAW IN OPPOSITION TO PLAINTIFFS' MOTION TO EXCLUDE OPINIONS OF ANTHONY FERRANTE

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. BACKGROUND 2

A. Mr. Ferrante's Internet Security Experience 2

B. Mr. Ferrante's Opinions 3

III. LEGAL STANDARD 7

IV. MR. FERRANTE'S OPINIONS ARE RELEVANT. 8

A. Security, Privacy, and Fraudulent and Malicious Ads Are Relevant to This Case. 10

B. Mr. Ferrante's Opinions Are Helpful to the Fact Finder. 15

V. MR. FERRANTE'S OPINIONS DEPEND ON HIS EXTENSIVE EXPERIENCE IN INTERNET SECURITY. 17

A. Mr. Ferrante Explained How His Experience in Internet Security Informed His Opinions. 18

B. Mr. Ferrante Need Not Be an Expert in Digital Advertising or Support His Opinions with Peer-Reviewed Articles for His Opinions to Be Admissible. 21

C. The Testimony of Plaintiffs' Expert, Professor Wenke Lee, Demonstrates the Reliability of Mr. Ferrante's Opinions. 23

D. The Cases Cited by Plaintiffs Do Not Support Mr. Ferrante's Exclusion. 24

VI. MR. FERRANTE DID NOT RELY ON "FIELD TESTING" DONE FOR THIS CASE IN FORMING ANY OF HIS OPINIONS. 25

CONCLUSION 26

TABLE OF AUTHORITIES

Page(s)

Cases

Allied Orthopedic Appliances Inc. v. *Tyco Health Care Grp. LP*,
592 F.3d 991 (9th Cir. 2010) 9

Ohio v. *Am. Express Co.*,
585 U.S. 529 (2018).....9

Andrews v. *Woody*,
2018 WL 2452177 (E.D. Va. May 31, 2018) 24

Berlyn, Inc. v. *Gazette Newspapers*,
223 F. Supp. 2d 718 (D. Md. 2002).....8

United States v. *Bynam*,
604 F.3d 161 (4th Cir. 2010) 7

Cont'l T.V., Inc. v. *GTE Sylvania Inc.*,
433 U.S. 36 (1977).....9

Copeland v. *Bieber*,
2016 WL 7079569 (E.D. Va. Sept. 8, 2016).....25

Daubert v. *Merrell Dow Pharms., Inc.*,
509 U.S. 579 (1993).....7

In re Dealer Mgmt. Sys. Antitrust Litig.,
581 F. Supp. 3d 1029 (N.D. Ill. 2022) 15, 17, 18

Deutsch v. *Novartis Pham. Corp.*,
768 F. Supp. 2d 420 (E.D.N.Y. 2011) 22

E. Claiborne Robins Co. v. *Teva Pharm. Indus., Inc.*,
2022 WL 3710758 (E.D. Va. Feb. 23, 2022).....16

Epic Games, Inc. v. *Apple, Inc.*,
67 F.4th 946 (9th Cir. 2023) 9

United States v. *Gasperini*,
2017 WL 3140366 (E.D.N.Y. 2017).....9, 15

Georges v. *Dominion Payroll Servs., LLC*,
2018 WL 2088751 (E.D. Va. May 4, 2018) 24

Goldwasser v. *Ameritech Corp.*,
222 F.3d 390 (7th Cir. 2000) 10

United States v. *Grinnell Corp.*,
384 U.S. 563 (1966) 8

Kiessling v. *Kiawah Island Inn Co. LLC*,
2019 WL 331176 (D.S.C. Jan. 25, 2019) 22

Kumho Tire Co. v. *Carmichael*,
526 U.S. 137 (1999) 7

Leegin Creative Leather Prods., Inc. v. *PSKS, Inc.*,
551 U.S. 877 (2007) 10

United States v. *Mallory*,
2018 WL 11438046 (E.D. Va. June 5, 2018) 7

Merritt v. *Old Dominion Freight Line, Inc.*,
2011 WL 322885 (W.D. Va. Feb. 2, 2011) 17

United States v. *Microsoft Corp.*,
253 F.3d 34 (D.C. Cir. 2001) 8

N.O. v. *Alembik*,
160 F. Supp. 3d 902 (E.D. Va. 2016) 22

Nix v. *Chemours Co.*,
2023 WL 6471690 (E.D.N.C. Oct. 4, 2023) 22

Oksanen v. *Page Memorial Hosp.*,
945 F.2d 696 (4th Cir. 1991) (en banc) 8

United States v. *Parkhurst*,
865 F.3d 509 (7th Cir. 2017) 17

FTC v. *Qualcomm Inc.*,
969 F.3d 974 (9th Cir. 2020) 9

Quality Plus Servs. v. *Nat'l Union Fire Ins. Co.*,
2020 WL 239598 (E.D. Va. Jan. 15, 2020) 18

Robinson v. *Nationstar Mortg. LLC*,
2019 WL 4261696 (D. Md. Sept. 9, 2019) 22

Robles v. *United States*,
2020 WL 8254267 (E.D. Va. Oct. 15, 2020) 24

S.A.S. Inst., Inc. v. *World Programming Ltd.*,
874 F.3d 370 (4th Cir. 2017) 17

Sines v. *Kessler*,
2021 WL 1431296 (W.D. Va. Apr. 15, 2021) 16

United States v. *Sullivan*,
2022 WL 3716594 (N.D. Cal. Aug. 28, 2022) 18

United States v. *Tejeda-Ramirez*,
259 F. App'x 535 (4th Cir. 2007) 15

The Harvester, Inc. v. *Rule Joy Trammel + Rubio, LLC*,
2010 WL 2653373 (E.D. Va. July 2, 2010) 22

Thomas M. Gilbert Architects, P.C. v. *Accent Builders & Devs., LLC*,
2008 WL 5552323 (E.D. Va. June 4, 2008) 15

Thompson Everett, Inc. v. *Nat'l Cable Advert., L.P.*,
850 F. Supp. 470 (E.D. Va. 1994) 8

Tyree v. *Boston Sci. Corp.*,
54 F. Supp. 3d 501 (S.D. W. Va. 2014) 22

Wiener v. *AXA Equit. Life Ins. Co.*,
481 F. Supp. 3d 551 (W.D.N.C. 2020) 7, 17

United States v. *Wilson*,
484 F.3d 267 (4th Cir. 2007) 17, 23

I. INTRODUCTION

With over two decades of experience in Internet security, including 12 years at the Federal Bureau of Investigation ("FBI") specializing in cybersecurity, there is no question that Mr. Ferrante is well-qualified. Plaintiffs are not challenging Mr. Ferrante's qualifications. Instead, Plaintiffs challenge the relevance and reliability of Mr. Ferrante's opinions. Because Internet security is a core issue in this case and Mr. Ferrante relies on his wealth of experience in Internet security, all of Plaintiffs' arguments should be rejected and their motion denied.

First, Mr. Ferrante's opinions are relevant. If Plaintiffs' antitrust claims survive summary judgment, Google is entitled to demonstrate that its product design decisions were not anticompetitive and instead have advanced legitimate and procompetitive benefits, such as security. Plaintiffs cannot challenge Google's product design decisions and at the same time prohibit Google from explaining the procompetitive and pro-consumer reasons for its decisions. Google has succeeded by product quality, including security for advertisers, publishers, and users. Plaintiffs are wrong when they suggest that security issues are irrelevant to competition among ad tech providers, which are a major target of bad actors and organized crime. Mr. Ferrante, based on his experience in Internet security, both in the public and private sectors, will explain the security threats facing the entire digital advertising ecosystem, including the increasing threat of organized crime.

Second, Plaintiffs ineffectually attack Mr. Ferrante's opinions because they do not rest on a scientific method; but, as the Advisory Committee Notes to Rule 702 explain, experience is "the predominant, if not sole, basis for a great deal of reliable expert testimony." Fed. R. Evid. 702. As Mr. Ferrante explained, the Internet protocol and related technologies are commonplace and not unique to digital advertising, and he has been investigating them for decades, both at the FBI and on behalf of private clients. That experience provides a reliable basis for his opinions. The

testimony of Plaintiffs' expert, Professor Wenke Lee, underscores this point. Professor Lee agreed with the core of Mr. Ferrante's opinions; to the extent that his opinions diverged, it was because his opinions were not grounded in real-world facts.

Finally, Plaintiffs make much of the so-called "field testing" performed by Mr. Ferrante. The "field testing" amounted to his signing onto a website for the benefit of his younger staff to show how information—both encrypted and unencrypted—traversed the Internet. The demonstration was no different than the thousands he performed prior to this engagement and did not inform any of his opinions.

Google respectfully requests that Plaintiffs' motion to exclude Mr. Ferrante's testimony be denied.

II. BACKGROUND

A. Mr. Ferrante's Internet Security Experience

Anthony Ferrante has held positions in Internet security, both in the public and private sectors, for his entire career. After obtaining an undergraduate degree and a master's degree in computer science, Mr. Ferrante joined the FBI where he held multiple positions, all relating to cybersecurity.

In 2005, he started as a special agent in the FBI's New York Field Office, and in 2006, he was selected to serve as a member of the FBI's Cyber Action Team, a team that deploys globally to respond to the most critical cyber incidents on behalf of the U.S. government. Ex. 101, ¶ 5.[1]

[1] All references to Exs. A and B refer to exhibits to Plaintiffs' Motion to Exclude Expert Testimony of Anthony Ferrante, ECF No. 589. All references to Ex. 1 through 126 refer to the Declaration of Bryon Becker in Support of Google LLC's Motion for Summary Judgment and Motions to Exclude, ECF No. 581, and Declaration of Bryon Becker in Support of Google LLC's Oppositions to Plaintiffs' Motions to Exclude. With respect to quoted material, unless otherwise indicated, all brackets, ellipses, footnote call numbers, internal quotations, and citations have been omitted for readability. All emphasis is added unless otherwise indicated.

From March 2014 to October 2015, Mr. Ferrante served as Chief of Staff for the FBI's Cyber Division, and from October 2015 to April 2017, he served as Director for Cyber Incident Response on the White House's National Security Council. *Id.* ¶¶ 5–6. During his tenure at the FBI, Mr. Ferrante oversaw cases relating to advertising fraud and malvertising and "saw a spike in the exploitation of the advertising ecosystem" as a "vector in which to target users." Ex. B, ECF. No. 589-2, February 20, 2024, Deposition of Anthony J. Ferrante ("Ferrante Dep.") at 22:8–18.

After he left the FBI, Mr. Ferrante became the Global Head of Cybersecurity at FTI Consulting. Mr. Ferrante has testified in several matters and regularly provides cybersecurity consulting services to Fortune 500 companies, including many technology companies. Ex. 101, ¶ 4 & App. A. In providing consulting services to private clients, Mr. Ferrante continues to work with the government in connection with cyber-related investigations. Ferrante Dep. at 264:4–16 (working on behalf of clients "cooperating with the government"). In addition, the consulting work he has done on behalf of clients has included being "called to assist organizations in big tech in response to bolstering advertising technologies." *Id.* at 272:17–273:7.

Based on his experiences in both government and the private sector, Mr. Ferrante has first-hand operational knowledge of more than 60 criminal and national security cyber threat sets and various groups of threat actors. Ex. 101, ¶ 4.

B. Mr. Ferrante's Opinions

Mr. Ferrante offers four opinions relating to Internet security, in the context of the digital advertising ecosystem. *First*, "malvertising and digital advertising fraud are now a persistent and pernicious form of organized crime, presenting a substantial threat to global Internet users and all participants in the digital advertising ecosystem and costing participants in the ecosystem billions of dollars every year." Ex. A, ECF No. 589-1, January 23, 2024, Expert Report of Anthony J. Ferrante ("Ferrante Rpt.") ¶ 8. As Mr. Ferrante explains in his report, ad fraud and malvertising

have become a preferred tool of organized crime. By next year, ad fraud is estimated to become organized crime's second-largest source of income, second only to drugs. *See id.* ¶ 16. This criminal activity is destructive, costing publishers and consumers millions of dollars and infecting millions of computers. *Id.* ¶¶ 16–18. For example, the 3ve criminal operation, which Google assisted in dismantling, resulted in 1.7 million personal computers being infected with malware, more than 1 million IP addresses being compromised, and nearly $30 million in wasted advertising dollars. *Id.* ¶ 58.

It is important to recognize that digital advertising interacts with sensitive private consumer information, including a user's IP address, cookies, and browser information; the domain and URL of the page and previous page loaded by the user; publisher-shared data on the user (*e.g.*, their gender, race, parents, income bracket, education, year of birth, zip code); and potential specific data on their interests (*e.g.*, movie bug, fitness enthusiast, pet lover). Ad fraud and malvertising often siphons or otherwise misappropriates such sensitive personal information. *Id.* ¶ 74.

Ad fraud also significantly reduces advertisers' return on their investment by diverting dollars away from real publishers through fake activity. *Id.* ¶ 10 (ad fraud is an "attempt to deceive advertising platforms into thinking that fake activity on the network is real user behavior for the purpose of financial gain"). By some estimates, it has cost publishers and advertisers $100 billion. *Id.* ¶ 24. Malvertising, or malicious advertising, results in malware being placed on a user's device or directing the user to a malicious website after the user clicks on what they think is a legitimate advertisement. *Id.* ¶ 11. Once malware is installed, it "can damage files, redirect Internet traffic, monitor the user's activity, steal data, or set up backdoor access points to the user's device. Malware may also delete, block, modify, leak or copy data, which can then be sold on the dark web, sold back to the user for ransom." *Id.* ¶ 12. Industry sources estimate that malvertising

impacts almost 1 in every 100 ad impressions generated and more than 20% of user sessions. *Id.* ¶ 13.

Plaintiffs' experts acknowledge the threat that ad fraud and malvertising pose to digital advertising. For example, Plaintiffs' security expert, Wenke Lee, admits that "fraud and malicious activity directed against digital advertising is a concern for advertisers, publishers, consumers, and other participants in the digital advertising ecosystem." Ex. 112, ¶ 12. These activities "can harm the integrity of online advertising campaigns, harm participants in the digital advertising ecosystem, skew performance metrics, and siphon advertising spending and profits away from honest and reputable participants in the system." *Id.* Similarly, Plaintiffs' marketing expert, Kenneth Wilbur, highlighted in a 2021 paper he co-authored about "Inefficiencies in Digital Advertising Markets" that "most industry estimates indicate that fraud takes 10%–30% of total digital advertising revenue." Ex. 113, at 2.

Second, "Google stood out as an early industry leader in the face of this rising threat. Google developed and collaborated with partners to set and invest in standards and protocols for industry-wide use to improve the entire advertisement ecosystem and make it safer for all participants, including through its role in developing ads.txt and collaborating with industry working groups such as the Interactive Advertising Bureau Technology Lab and Trustworthy Accountability Group." Ferrante Rpt. ¶ 8.

Third, the "open environment that the header bidding auction method provides, and its lack of integration between exchanges and its participants, creates opportunities for malicious actors to take advantage of Internet users and advertisers." *Id.*[2] Mr. Ferrante explained that the rise of

[2] "Header bidding is a programmatic auction in which publishers send bid requests to multiple demand partners in real time outside of their primary ad server." Ferrante Rpt. ¶ 66.

header bidding created additional opportunities for fraudulent activity, particularly in the form of domain spoofing when the industry standard, ads.txt, had not yet been adopted. *Id.* ¶¶ 50–52, 66–71.

Fourth, "Google's development of the Open Bidding methodology and its integrated environment enabled Google to bolster security through the application of its tools and standards at all ends of the process." *Id.* ¶ 8. Google began to introduce Open Bidding in 2016, and, in contrast to header bidding as it then existed, it provided "bidding over Google's servers, as opposed to through code embedded in the publisher's page." *Id.* ¶ 77. "Open Bidding requests occur through a server-to-server integration" so that "instead of bidding through page tags and via browsers on the user's device, bidding takes place on the ad server, resulting in increased security." *Id.*

Mr. Ferrante explained that Open Bidding addressed "six points" that were prevalent in header bidding:

> Open bidding is a framework developed by Google that, you know, closed a lot of the gaps and mitigated a lot of the risks that I spoke about earlier today. It did away with man-in-the-middle attacks on the wire. The sensitive user data was passed by encrypted communications. It did away with the listening in plain sight to non-legitimate players in the bidding process. It did away with the ability for malicious actors to buy access to users' machines. It spearheaded the effort with partners in the industry to come up with the ads technology, ads.txt framework. It created a know-your-customer program, a vetting process. And then, again, with those technologies, it helped stop the essential competitive intel collected on peers in the bidding process.

Ferrante Dep. at 235:4–20. Mr. Ferrante further explained that these features in Open Bidding "were very quickly adopted by others in the industry" who "applied them in the header bidding framework." *Id.* at 235:21–236:2.

III. LEGAL STANDARD

The Federal Rules contemplate a broad view of expert qualifications. The text of Rule 702 expressly states that an expert may be qualified on the basis of experience. Fed. R. Evid. 702 ("A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion"). "Inasmuch as the rule uses the disjunctive, a person may qualify to render expert testimony in any one of the one five ways listed: knowledge, skill, experience, training, or education." *Wiener* v. *AXA Equit. Life Ins. Co.*, 481 F. Supp. 3d 551, 558 (W.D.N.C. 2020) (quoting *Kopf* v. *Skym,* 993 F.3d 374, 377 (4th Cir. 1993)). In many instances, experience is "the predominant, if not sole, basis for a great deal of reliable expert testimony." Fed. R. Evid. 702 advisory committee's note to 2000 amendments; *see Daubert* v. *Merrell Dow Pharms., Inc.*, 509 U.S. 579, 592 (1993) (expert witnesses testimony is given latitude unavailable to other witnesses on the "assumption that the expert's opinion will have a reliable basis in the knowledge and experience of his discipline").

As the Supreme Court has explained, "the relevant reliability concerns may focus upon personal knowledge or experience" for a non-scientific expert. *Kumho Tire Co.* v. *Carmichael*, 526 U.S. 137, 150 (1999). Although "experiential expert testimony does not rely on anything like a scientific method, such testimony is admissible under Rule 702 so long as an experiential witness explains how his experience leads to the conclusion reached, why his experience is a sufficient basis for the opinion, and how his experience is reliably applied to the facts." *United States* v. *Bynam*, 604 F.3d 161, 167-68 (4th Cir. 2010); *see also United States* v. *Mallory*, 2018 WL 11438046, at *1 (E.D. Va. June 5, 2018) (denying *Daubert* challenge to experts' testimony as to the general document classification processes and classification decisions at issue in the case based on experts' "many years of experience in classifying information and documents within the U.S. Intelligence Community").

IV. MR. FERRANTE'S OPINIONS ARE RELEVANT.

Security is a critical issue for digital advertising. Failure to actively police ad fraud and malvertising costs publishers and advertisers billions of dollars and places consumers in harm's way. Plaintiffs nonetheless attempt to argue that security issues are not relevant to this case. Plaintiffs' relevancy arguments seek to attack Google's product design choices and, at the same time, exclude Google's procompetitive and pro-consumer reasons for those choices.

Should Plaintiffs survive summary judgment, they will have to prove, in part, that Google "willfully" acquired or maintained monopoly power in each of the three alleged product markets. *See United States* v. *Grinnell Corp.*, 384 U.S. 563, 570–71 (1966). To satisfy the element of willfulness, Plaintiffs must prove that Google had "no valid business reason or concern for efficiency" when engaged in the challenged conduct. *Oksanen* v. *Page Memorial Hosp.*, 945 F.2d 696, 710 (4th Cir. 1991) (en banc); *accord Berlyn, Inc.* v. *Gazette Newspapers*, 223 F. Supp. 2d 718, 735 (D. Md. 2002); *Thompson Everett, Inc.* v. *Nat'l Cable Advert., L.P.*, 850 F. Supp. 470, 482 & n.12 (E.D. Va. 1994).

Moreover, where a burden-shifting framework applies, "the plaintiff, on whom the burden of proof of course rests must demonstrate that the monopolist's conduct indeed has the requisite anticompetitive effect," "that is, it must harm the competitive *process* and thereby harm consumers." *United States* v. *Microsoft Corp.*, 253 F.3d 34, 58–59 (D.C. Cir. 2001). If a "plaintiff successfully establishes a *prima facie* case under § 2 by demonstrating anticompetitive effect, then the monopolist may proffer a procompetitive justification for its conduct." *Id.* at 59. Conduct is procompetitive if it "is indeed a form of competition on the merits because it involves, for example, greater efficiency or enhanced consumer appeal." *Id.* If the defendant offers a procompetitive justification, the burden shifts back to the plaintiff to rebut it. *Id.* Finally, "if the monopolist's procompetitive justification stands unrebutted, then the plaintiff must demonstrate that the

anticompetitive harm of the conduct outweighs the procompetitive benefit." *Id.*; *accord FTC* v. *Qualcomm Inc.*, 969 F.3d 974, 991 (9th Cir. 2020); *see also Ohio* v. *Am. Express Co.*, 585 U.S. 529, 541–42 (2018) (applying essentially the same burden-shifting framework under Section 1 of the Sherman Act).

In determining whether conduct is anticompetitive in the first step, it is "of no legal import" that a firm is accused of "a form of technological predation because a monopolist has the right to redesign its products to make them more attractive to buyers." *Allied Orthopedic Appliances Inc.* v. *Tyco Health Care Grp. LP*, 592 F.3d 991, 999 (9th Cir. 2010). Further, the protection of advertisers, publishers, and Internet users from security threats and privacy violations is a well-established procompetitive rationale. *E.g., Cont'l T.V., Inc.* v. *GTE Sylvania Inc.*, 433 U.S. 36, 55 & n.23 (1977) ("safety and quality of products" are legitimate business justifications for a firm's conduct); *Epic Games, Inc.* v. *Apple, Inc.*, 67 F.4th 946, 987 (9th Cir. 2023) (security and privacy are cognizable procompetitive rationales).[3]

In cases outside the antitrust context, the U.S. government has introduced expert testimony on Internet security topics. For example, in *United States* v. *Gasperini*, 2017 WL 3140366, at *2 (E.D.N.Y. 2017), the court overruled objections to the government's expert witness on "general terminology relating to cybercrime, including botnets, click fraud scripts, malware and other terms." The court held that while "the proffered expert testimony here does not directly implicate the allegations against Defendant, it provides background regarding the sometimes obscure

[3] Plaintiffs may argue that Google's business justifications are "pretextual"; Google is entitled to rebut that argument. Mr. Ferrante's opinions are relevant not only to Google explaining its "valid business reasons" for its product design decisions, but also for rebutting any argument that its business justifications are "pretextual."

technology and concepts at issue in the case, including malware, botnets, and server operations, and other terms that are likely to be unfamiliar to the average juror." *Id.*

A. Security, Privacy, and Fraudulent and Malicious Ads Are Relevant to This Case.

Ad tech's ability to ensure security and privacy for its advertisers, publishers, and Internet users is highly relevant to the competition issues in this case. Central to Google's defense is that it has competed vigorously, including through design choices to ensure product quality, safety, and privacy. *Leegin Creative Leather Prods., Inc.* v. *PSKS, Inc.*, 551 U.S. 877, 896–97 (2007) (antitrust laws permit a manufacturer to strive "to improve its product quality"); *Goldwasser* v. *Ameritech Corp.*, 222 F.3d 390, 397 (7th Cir. 2000) ("even a monopolist is entitled" to improve the "quality of its products"). Plaintiffs maintain that it is Google's alleged anticompetitive conduct that has caused its success, not the quality of Google's products. *E.g.*, First. Am. Compl. ECF No. 120 ("FAC") ¶¶ 262–65. The quality of Google's ad tech, including its ability to prevent digital ad fraud, is thus directly relevant to its defense of this case. A key method by which Google competes is to provide quality ads and quality inventory—i.e., free from fraud and malware. *E.g.*, Ex. 126, at -051 ("Lack of trust in DCLK spam defenses may divert spend to competitors"); Ex. 122, at -545 ("Creating a Competitive Advantage for AdX through Clean Ad Traffic"); Ex. 125, at -264 ("Google Adwords has a rigorous, human-led certification process for third-party partners that can serve or measure ads on AdWords . . . and DoubleClick Ad Exchange"); *id.* at -265 ("The advertising industry has a long history of bad actors looking to profit from invalid traffic, ad fraud, misrepresentative content and more. Google takes its role very seriously in combating bad actors by constantly making improvements to protect the integrity of our systems and our users' security"). Google's competitors likewise recognize that clean and safe ads and ad inventory are paramount to a successful business. *E.g.*, Ex. 115 at 27:10–14 ("ensuring that we don't work with

publishers that would not adhere to what we consider critical for good user value, i.e., no fraud, no spam, no porn, no illegal stuff, is key"); Ex. 117 at 307:12–16 ("Q. During your time at AppNexus, Mr. O'Kelley, was protecting against fraud, ad fraud a major competitive concern? A. Yes."). In comparing prices of ad tech in this case, Plaintiffs' experts acknowledge that those prices must be compared on a quality-adjusted basis, Ex. 1, ECF No. 597-1 ¶ 248 & n.335, and yet Plaintiffs ask the Court to ignore and block evidence on this key product quality feature of security.

Ad tech providers such as Google who own multiple products in the ad tech stack can deliver more secure and higher-quality services and products. Google's expert economist Dr. Mark Israel has explained that the "procompetitive incentives generated by Google's integration" of its ad tech include protecting the open web ecosystem against fraud, spam, and other forms of abuse. Ex. 118, ¶ 55. Google's competitors acknowledge the security benefits allowed by owning and integrating multiple ad tech products. Ex. 104 at 93:22–94:18 (explaining that Meta's control of "wholly-owned apps and services" gives it a "very high degree of confidence of being able to police or monitor spam and fraud"); Ex. 116 at 289:13–20 ("Q. And if you look down, it refers to the Xandr's end-to-end platforms? A. That is correct. Q. And would you agree that having an end-to-end platform helps prevent fraud? A. Yes.").

Google's expert economist Dr. Mark Israel has opined on how Plaintiffs' position that Google must share its innovations with rivals would undermine the notable investments that Google has made to offer high-quality products. Ex. 118, ¶¶ 500, 518–19. Google's investments into the security and privacy of ad tech, excluding machine costs, have risen dramatically from $36 million in 2017 to more than $180 million in 2022. *Id.* ¶ 131 & Fig. 6. Google blocks billions of ads that violate its policies, including millions of cases of adult or inappropriate content, misrepresentation, and dangerous products or services, and has taken action against millions of

pages that include cases of "malicious or unwanted software," "sexual content," and other "shocking content." Ferrante Rpt. ¶¶ 47-48.

Security issues also relate directly to Plaintiffs' claims of specific alleged anticompetitive conduct. Plaintiffs' theory as to why certain conduct is anti-competitive rests on Google's decision not to establish innumerable technical connections to countless exchanges and servers. *E.g.*, Ex. 6, ECF No. 581-6 at 89:13–90:4; Ex. 32, ECF No. 583-2 at 100:11–102:16. The interoperability that Plaintiffs seek would actually make Google's products less secure. But according to Plaintiffs, competition requires completely open environments on Google's ad tech tools, accessible by third parties and rivals, notwithstanding the substantial security risks. *E.g.*, Ferrante Rpt. ¶¶ 8, 14–24.

Product quality through safety and security features is at the forefront of the product design decisions that Plaintiffs challenge:

Gradual Access to Google Ads' Advertiser Demand: Plaintiffs claim that Google acted anticompetitively by providing "unrestricted access to Google Ads' advertiser demand exclusively to its AdX ad exchange, and denying comparable access to rival ad exchanges." Ex. 1, ECF No. 597-1 ¶ 12(3)(1). Under Plaintiffs' theory, all Google advertisers should have been available to all exchanges. Providing competitor exchanges unrestricted access to Google Ads advertising customers, which Plaintiffs insist should have happened years ago, would have created major security issues. In 2013, Google gradually began making those advertisers available to other exchanges through a product innovation known as AwBid, without sacrificing safety and quality for Google Ads advertiser customers. Under Plaintiffs' theory, unfettered access to all Google Ads advertisers should have been available to all exchanges.

When Google first introduced AwBid, even on a limited basis, to connect its customers to other exchanges, Google found that a number of the other exchanges did not "have the same

rigorous spam detection mechanism in place as Google does." Ex. 119 at -469; *see also id.* (finding that AwBid had a 10%–70% spam click rate whereas AdX was only 7%–8%). AwBid inventory was also flagged for harmful content including "Pedophilia," "Gore," "Fight Videos," and "Nudity/Porn." Ex. 120 at -439. This was the result of being beholden to the security features (or lack thereof) of the third-party exchanges on AwBid. Google's decision to allow gradual access to third-party exchanges over time is explained in part by the existence of these serious security risks and the need for Google to address them.

Comparable Access by Publisher Ad Servers to AdX: Plaintiffs contend that Google should provide the same or similar AdX access to rival publisher ad servers. Ex. 1, ECF No. 597-1 ¶ 12(3)(2). Providing comparable AdX access to third-party publisher ad servers presents security risks. *E.g.*, Ex. 123 at -283 ("How to authenticate 3PAS? Establishing a SSL connection for each ads request is probably too expensive. Without SSL, a hacker could easily sniff the packet from 3PAS to AdX, and even worse, impersonate a 3PAS, request lots of impressions without ever displaying any."); Ex. 49, ECF No. 584–9 at -665 ("engineering concerns associated with spam detection and inventory quality controls").

Third-Party Exchange Access to AdMeld: Plaintiffs maintain that following the acquisition of AdMeld, Google should have integrated an AdMeld feature (which enabled AdMeld's ad exchange to provide real-time bids to third-party ad servers) into Google's ad tech stack. Ex. 1, ECF No. 597-1 ¶ 12(3)(5); Ex. 3, ECF No. 597-3 ¶ 686; Ex. 6, ECF No. 581-1 at 286:5–17, 288:7–12, 295:4–296:1; Ex. 8, ECF No. 597-7 at 290:4–14, 292:5–293:1; Ex. 44, ECF No. 600-1 ¶ 69; Ex. 2, ECF No. 597-2 ¶¶ 116, 382. This technical integration with third party-exchanges again raised important security issues. Ex. 48, ECF No. 584-8 at -004 ("Support Costs and Risks for Google": "Account managers and the spam team will have a new type of spam to manage").

Plaintiffs allege Google's decision not to integrate that feature was anticompetitive. But valid business reasons, such as security concerns, explain why, as with other technical decisions that Plaintiffs maintain Google should have made, Google ultimately did not incorporate that AdMeld feature.

Introduction of Open Bidding in Response to Header Bidding: Plaintiffs criticize Google's decision not to participate in header bidding and instead develop a competing product known as Open Bidding. FAC ¶ 184. Header bidding, as open-source code on a publisher website, potentially exposes private consumer information to unknown header bidder auctions, a well-known security threat. Ferrante Dep. at 185:4–186:10. With header bidding, "Each and every bidder receives the data about the users who will be served an ad, leading to multiple opportunities for data leaks." Ferrante Rpt. ¶ 74; *see also* Ex. 124 at -946 ("Cons" of Header Bidding include "Data Security/leakage" and "risk of bid fraud").[4]

As competitors recognized, Google responded to header bidding with Open Bidding in part due to fraud concerns. Ex. 35, ECF No. 599-4 at -048 ("The container/header bidding explosion of 2016 created a lot of opportunity for malfeasance that has been covered in the press. Rather than fight against the container/header bidding trend, Google recognized it was in the best interests of its customers to offer a competing solution –" Open Bidding. "Google wanted its solution to be clear of the fraud and malfeasance.").

"Last Look": Plaintiffs complain that the design of Google's technology gave Google a "Last Look" as the result of header bidding auctions rather than permitting header bidding to bid alongside Google customers on AdX. Ex. 1, ECF No. 597-1 ¶ 12(3)(5). Plaintiffs maintain that

[4] Ross Benes, *Unraveling header bidding's problems with user data*, DigiDay (Mar. 20, 2017), https://digiday.com/media/header-bidding-security/ ("There are some real security concerns about header bidding that aren't being talked about").

Google should have redesigned DFP to allow publishers to give rival exchanges a "last look," Ex. 6, ECF No. 581-6 at 272:7–273:22, 280:3–281:4; Ex. 2, ECF No. 597-2 ¶¶ 345–349, or to submit real-time bids alongside AdX in an attempt to beat the winning bid from the header bidding auction, Ex. 2, ECF No. 597-2 at 278:9- 282:11; Ex. 32, ECF No. 583-2 at 130:24-131:13; Ex. 1, ECF No. 597-1 ¶ 673. Doing so would have introduced the concerns described above because header bidding would be bidding alongside AdX bidders.

B. Mr. Ferrante's Opinions Are Helpful to the Fact Finder.

Given the importance of security, privacy, and fraud issues in this case, Mr. Ferrante's testimony provides obvious background on issues on which the jury will not be well versed. *Gasperini*, 2017 WL 3140366, at *2. The sole case that Plaintiffs cite in support of their relevance argument, *Thomas M. Gilbert Architects, P.C.* v. *Accent Builders & Devs., LLC*, 2008 WL 5552323, at *1 (E.D. Va. June 4, 2008), is a two-paragraph order granting summary judgment on some claims and excluding "any part of the expert's testimony that is not relevant to the remaining issues" in the case. In contrast, here, Mr. Ferrante's testimony will be helpful to the fact finder's evaluation of the security concerns influencing Google's product design and business decisions. *E.g.*, *In re Dealer Mgmt. Sys. Antitrust Litig.*, 581 F. Supp. 3d 1029, 1084 (N.D. Ill. 2022) (denying motion to exclude cybersecurity expert offering opinions on "security concerns" faced by defendants and "security issues posed by hostile DMS access"). In particular, Mr. Ferrante's testimony regarding organized crime's role in proliferating digital advertising fraud and malvertising is especially useful and relevant for the jury. *E.g.*, *United States* v. *Tejeda-Ramirez*, 259 F. App'x 535, 538 (4th Cir. 2007) (techniques used in drug trafficking were the proper subject of expert testimony); *Sines* v. *Kessler*, 2021 WL 1431296, at *6–7 (W.D. Va. Apr. 15, 2021) ("Expert testimony is also allowed when it provides the jury background on the history, structure,

leaders, or operations of an unfamiliar organization or subculture, as that information often can further situate communications and other relevant evidence into context.").

Mr. Ferrante's opinions concerning Google being a "leader" in addressing security issues in connection with digital advertising is likewise relevant to the competition issues in this case. For example, Google helped to lead the way in the development and adoption of key industry standards that made the entire digital advertising ecosystem safer. *Cf. E. Claiborne Robins Co.* v. *Teva Pharm. Indus., Inc.*, 2022 WL 3710758, at *4 (E.D. Va. Feb. 23, 2022) (permitting expert testimony "on general pharmaceutical industry standards" as it "would aid the jury without invading the province of the jury or the court"). Mr. Ferrante can explain the impact of the industry standard known as "ads.txt," which was a Google-led initiative that allowed advertising platforms to verify inventory and publisher relationships; it played a key role in reducing domain spoofing exacerbated by header bidding. Ferrante Rept. ¶¶ 50–52. Google's role in developing these standards and its collaboration with law enforcement to take down criminals underscore the importance of security and its relevance to how Google competes and succeeds.

Finally, Mr. Ferrante's third and fourth opinions concerning header bidding and Open Bidding are relevant; Plaintiffs, in an entire section of their Amended Complaint, allege that Google acted anticompetitively by not providing immediate and easy access to header bidding. FAC § IV.D. Mr. Ferrante's testimony will help the fact finder understand the security risks posed by header bidding as well as the security benefits of Google's Open Bidding. For example, Mr. Ferrante can explain how Google's integrated approach with Open Bidding allowed it to "implement data privacy measures" that prohibit malware and other dangerous content. Ex. A, ¶ 78. Contrary to Plaintiffs' argument, this testimony is relevant and helpful to the fact finder, even if Mr. Ferrante is also not offering a direct comparison of the security of Google's products

with that of others. *E.g.*, *In re Dealer Mgmt. Sys. Antitrust Litig.*, 581 F. Supp. 3d at 1084–85 (denying motion to exclude cybersecurity expert who "did not assess the use of APIs by other DMS providers").

V. MR. FERRANTE'S OPINIONS DEPEND ON HIS EXTENSIVE EXPERIENCE IN INTERNET SECURITY.

"Where, as here, the expert's opinion is grounded in experience in a particular field, courts will generally not preclude his testimony merely because it is not tested, subject to peer review and publication, or has no known rate of error." *Merritt* v. *Old Dominion Freight Line, Inc.*, 2011 WL 322885, at *5 (W.D. Va. Feb. 2, 2011); *see also Wiener*, 481 F. Supp. 3d at 558–60 (rejecting argument that expert's testimony should be excluded because "he did not use a recognized methodology in forming his opinions" where expert's opinions was based on his underwriting experience). An expert does not need a methodology—beyond his experience—for his opinions to be admissible. Experiential testimony is admissible as long as the expert is able to "explain how his experience leads to the conclusion reached, why his experience is a sufficient basis for the opinion, and how his experience is reliably applied to the facts." *United States* v. *Wilson*, 484 F.3d 267, 274 (4th Cir. 2007); *see also S.A.S. Inst., Inc.* v. *World Programming Ltd.*, 874 F.3d 370, 384 (4th Cir. 2017) ("Storer relied on his experience to inform his testimony, rather than any particular scientific method. The district court concluded that Storer's education and experience in software development qualified him as an expert in this matter."); *United States* v. *Parkhurst*, 865 F.3d 509, 516 (7th Cir. 2017) ("Training and experience are proper foundations for expert testimony").[5]

[5] Plaintiffs' expert, Prof. Wenke Lee, for his method, said that he relied on the "five-step principles": "first describe, you know, what problem you are addressing, what are the different factors of this—aspects of this problem that would lead you to believe how effective technology should be. I then describe, okay, here is the technology that I used to address this problem, including some of the existing technologies. And they you say, okay, and then you arrive at some meaningful results for people to evaluate the effectiveness of the technology." Ex. 114 at 67:13–68:4. Prof. Lee was unable to identify any textbook or article that set forth his "five-step

Courts have approved cybersecurity experts testifying based on their experience against *Daubert* challenges in a number of cases. *E.g.*, *In re Dealer Mgmt. Sys. Antitrust Litig.*, 581 F. Supp. 3d at 1084–85 (denying *Daubert* challenge to cybersecurity expert); *Quality Plus Servs.* v. *Nat'l Union Fire Ins. Co.*, 2020 WL 239598, at *15–16 (E.D. Va. Jan. 15, 2020) (denying *Daubert* challenge to cybersecurity expert who "did not perform tests to arrive at his opinions, instead relying on his expertise"); *United States* v. *Sullivan*, 2022 WL 3716594, at *23 (N.D. Cal. Aug. 28, 2022) (denying *Daubert* challenge to government cybersecurity expert who "applied his experience to the facts").

A. Mr. Ferrante Explained How His Experience in Internet Security Informed His Opinions.

Mr. Ferrante's experience in Internet security—both during his 12 years at the FBI and in private practice providing consulting services on cybersecurity issues, including incident response—informs his opinions and provides an appropriate foundation for his opinions. Mr. Ferrante's opinion concerning the extent to which malvertising and advertising fraud are threats is based on his investigation of cyber-related crimes while at the FBI and in consulting private clients in cyber-related issues and incident response. While at the FBI he "saw malvertising as a vector that was being exploited in increasing volume." Ferrante Rpt. ¶ 17; *see also* Ferrante Dep. at 23:25–24:4 ("when I arrived in 2005 through my time in the New York City field office, it was most certainly a vector that was being exploited, similar to that of spam e-mail and phishing email"); *id.* at 25:17–22 ("I remember sitting down with organizations, talking to them about how advertisements can be exploited and drive-by-downloads can happen and spoof domains can occur for the facilitation of these criminal activities"). Mr. Ferrante also briefed members of Congress

---

principles." *See also id.* at 280:20–22 ("Like I said, it's a basic thing. Just like one plus one equals two. I don't know where you can look it up"); *id.* at 283:22–284:11.

concerning domain spoofing and malvertising and "the threats to the ecosystem." *Id.* at 47:23–48:15.[6]

Mr. Ferrante's opinion that Google was "an early industry leader" in responding to the threats of malvertising and ad fraud was also informed by his government service and his work in private practice. Ferrante Rpt. ¶ 8. Mr. Ferrante, in reaching his conclusion, identified multiple instances where Google took actions that made the advertising ecosystem safer and then brought along the entire industry. First, Google detected and played a leading role in the takedown of 3ve, "one of the most massive and complex fraud operations in digital advertising." Ferrante Rpt. ¶ 8; Ferrante Dep. at 278:3–12. Second, Google was instrumental in developing standards like ads.txt and then "led the charge" in promoting widespread adoption. Ferrante Dep. at 278:13–16. Third, Google developed Open Bidding, with the features of Open Bidding then being adopted in server-side header bidding. *Id.* at 285:22–287:9. Mr. Ferrante explained:

> Google is at the forefront. They are the leaders in this space and they are saying, hey, everybody, come with us, let's knowledge share, let's share information, let's work together. I mean, it is the exact concept the U.S. government wants, right, and it is the exact concept that I think the industry wants.
>
> The industry is not going to adopt technologies that one person in a vacuum develops. They want to coalesce around an idea and crowdshare it and make it the very best it can through knowledge sharing, and that's exactly what Google is doing. And they did it so well that ads.txt was widely adopted almost immediately and endorsed by IAB.

[6] In their motion, Plaintiffs emphasize that Mr. Ferrante could not provide details concerning the number of investigations he worked on concerning malvertising or ad fraud while at the FBI. He explained that investigations "are not as simple as we see this person exploited the advertising ecosystem and has targeted this entity or these groups of users. What we see is we see the victimization of end users, and that is what generates or initiates an investigation." Ferrante Dep. at 24:9–23.

Id. at 278:22–279:11; *see also id.* at 288:7–13 ("As the—as I said earlier, the greatest compliment or indicator that they're viewed as a leader is everyone else in the industry adopted their innovation, their approach, and it is now widely used in server side header bidding.").

Mr. Ferrante's opinions concerning the header bidding framework, as it existed when it was first adopted in the 2014–2015 time period, and Google's Open Bidding framework were based on breaking both frameworks into their constituent parts and applying his experience in Internet security to each part. *Id.* at 213:9–12 ("So we talk about header bidding, and when you take bits—you take the pieces that make up header bidding, and you take them apart, you understand the technologies."). When header bidding was first adopted, for example, it used cleartext communication as opposed to encrypted communication. *Id.* at 238:13–239:1. Based on his experience in Internet security, Mr. Ferrante explained the risks of cleartext communication, which he had exposure to both at the FBI and as a consultant on Internet security in private practice. As he explained:

> You are talking about a concept on the Internet that has existed for what, 25, 30 years. Of course it's well-documented that clear text communication is susceptible to eavesdropping. Why do you think the credit card industry moved to encrypted communication? Why do you think the U.S. government uses encrypted communications to communicate sensitive data? Because clear text communication is susceptible to collection and eavesdropping.

Id. at 218:16–219:1.

Mr. Ferrante's assessment of header bidding in the 2014–2015 time frame, based on his experience in Internet security, was consistent with that of other industry participants. For example, the Chief Technology Officer of the Interactive Advertising Bureau ("IAB") Tech Lab, a non-profit organization that develops "foundational technology and standards that enable growth

and trust in the digital media ecosystem,"[7] identified the same issues as Mr. Ferrante: "Header bidding led to publishers being more promiscuous in their demand partnerships, and more willing to turn to demand partners, which made it easier for bad actors to hide amongst all the activity." Ferrante Rpt. ¶ 70.

B. Mr. Ferrante Need Not Be an Expert in Digital Advertising or Support His Opinions with Peer-Reviewed Articles for His Opinions to Be Admissible.

Both in their motion to exclude Mr. Ferrante's testimony and at his deposition, Plaintiffs focus on whether Mr. Ferrante was able to identify specific companies who provided publisher ad servers or ad exchanges. That is not the relevant inquiry. Mr. Ferrante applied his experience in Internet security to digital advertising, with many of the technologies used in digital advertising being "commonly used Internet technologies." As Mr. Ferrante explained:

> A. I'm an expert in Internet security, networking. And what I'm telling you is the technologies are basic, basic common, commonly used Internet technologies. They're the same protocols, TCPIP, right. It's the same protocol that is used to push data from a website to, for example, an ad exchange. TCPIP. TCPIP scrambles the data, reconfigures the data, and then on the other end they read it. That data, if not encrypted is susceptible to eavesdropping.
>
> Q. Do you consider yourself an expert in digital advertising technology?
>
> A. I consider myself an expert in security and in this case how it is applied to the digital advertising space.

Ferrante Dep. at 219:13–220:6.

"Generally, the test for exclusion is a strict one, and one knowledgeable about a particular subject need not be precisely informed about all details of the issues raised in order to offer an

[7] IAB, *About the IAB Tech Lab* (accessed May 16, 2014), https://iabtechlab.com/about-the-iab-tech-lab/.

opinion." *Kiessling* v. *Kiawah Island Inn Co. LLC*, 2019 WL 331176, at *4 (D.S.C. Jan. 25, 2019) (quoting *Thomas J. Kline, Inc.* v. *Lorillard, Inc.*, 878 F.2d 791, 799 (4th Cir. 1989)); *see also Deutsch* v. *Novartis Pham. Corp.*, 768 F. Supp. 2d 420, 425 (E.D.N.Y. 2011) ("If the expert has educational and experiential qualifications in a general field closely related to the subject matter in question, the court will not exclude the testimony solely on the ground that the witness lacks expertise in the specialized areas that are directly pertinent." (citation omitted)). In addition, "gaps in an expert's knowledge generally go to the weight of the witness's testimony, not its admissibility." *N.O.* v. *Alembik*, 160 F. Supp. 3d 902, 908 (E.D. Va. 2016).[8]

Throughout their motion, Plaintiffs emphasize that Mr. Ferrante did not identify peer-reviewed journals that support his opinions. Mr. Ferrante's opinions should not be excluded because he does not rely on peer-reviewed literature for his opinions; "peer-reviewed literature is merely one tool an expert witness can use to support his or her opinion." *Tyree* v. *Boston Sci. Corp.*, 54 F. Supp. 3d 501, 568 (S.D. W. Va. 2014); *see also The Harvester, Inc.* v. *Rule Joy Trammel + Rubio,* LLC, 2010 WL 2653373, at *2 (E.D. Va. July 2, 2010) (rejecting argument that architect's testimony based on experience was inadmissible because his "method had not been tested, or subject to peer review and publication, and does not have a known rate of error"); *Robinson* v. *Nationstar Mortg. LLC*, 2019 WL 4261696, at *14 (D. Md. Sept. 9, 2019) ("The fact that Oliver's methodology has not been subjected to peer review and that he has not published any articles does not invalidate it.").[9]

[8] Plaintiffs also argue that Mr. Ferrante did not review any deposition testimony and cited only a limited number of documents produced in discovery. "The decision to not examine certain evidence goes to the weight of the opinion, not its admissibility." *Kiessling*, 2019 WL 331176, at *5 ("KIIC points to no case law that says an expert is required to consider all facts in a case when forming his opinion.").

[9] *See also Nix* v. *Chemours Co.*, 2023 WL 6471690, at *13 (E.D.N.C. Oct. 4, 2023) (denying motion to exclude expert explaining, "It is unclear, however, that Gamble's analysis would ever

C. The Testimony of Plaintiffs' Expert, Professor Wenke Lee, Demonstrates the Reliability of Mr. Ferrante's Opinions.

"A district court's reliability determination does not exist in a vacuum, as there exist meaningful differences in how reliability must be examined with respect to expert testimony that is primarily experiential in nature as opposed to scientific." *Wilson*, 484 F.3d at 274. Plaintiffs have offered no evidence in the record that refutes Mr. Ferrante's opinions. To the contrary, Mr. Ferrante not only sufficiently explained how his experience informed his opinions, the opinions of Plaintiffs' expert, Prof. Wenke Lee, support the opinions offered by Mr. Ferrante.

In providing examples of Google's leadership in making the digital ecosystem more secure, Mr. Ferrante identified the role that Google played in developing industry standards to address malvertising and ad fraud, such as ads.txt. Ferrante Rpt. ¶¶ 49–52. Prof. Lee acknowledged the importance of the standards that Google was instrumental in developing. In his report, he stated:

> Publishers and advertisers rely on the effective and readily available countermeasures to counteract any potential tendency of Header Bidding to reduce the security of their platforms. These include, for example, widely adopted industry standards such as ads.txt as well as app-ads.txt, sellers.json, and OpenRTB SupplyChain, all of which are useful in preventing fraud by allowing publishers, resellers and advertisers in a bidding transaction to verify and confirm each other's identities.

Ex. 112, ¶ 109. Prof. Lee agreed that the combination of these four standards made header bidding safer. Ex. 114 at 181:5–8 ("Q. Did the combination—did the adoption of these four standards make header bidding safer? A. Yes, I think so, yes.").

But, unlike Mr. Ferrante, Prof. Lee did not know when the use of header bidding first became widely adopted in relation to the standards that he said made header bidding safer. *Compare* Ferrante Rpt. ¶ 66 (explaining header bidding "became widely adopted by

---

be subject to academic peer review. Gamble has experience creating reports for corporations investing in real estate, not writing academic articles.").

publishers in 2014 and 2015, before ads.txt was developed and became an industry standard"), *with* Ex. 114 at 208:2–8 ("Like I said, I'm not checking specific timelines. That was not actually relevant to my – the task of analyzing Mr. Ferrante's report, per se. But I would say if I remember right, I think by 2018, you know, Header Bidding was starting to be adopted."). Nor did he know that Google first introduced Open Bidding—to provide a more secure alternative to header bidding—before the introduction of any of the standards that he concluded made header bidding safer. Ex. 114 at 181:16–182:1, 184:16–22, 210:4–19.

D. The Cases Cited by Plaintiffs Do Not Support Mr. Ferrante's Exclusion.

None of the cases that Plaintiffs cite support their request to preclude Mr. Ferrante from testifying. Significantly, Plaintiffs do not challenge Mr. Ferrante's extensive experience in Internet security or that he was applying that experience to evaluate security issues with common Internet technologies that were being used for the purpose of digital advertising, or come forward with any evidence, including testimony by their own expert, that Mr. Ferrante's opinions were unreliable. Plaintiffs attack his opinions because he did not have a subspecialty in security issues relating to digital advertising and did not cite peer-reviewed articles in support of his opinions. As explained above, that is not the applicable standard for exclusion.

Plaintiffs' cases involved expert reports that were so perfunctory they did not even comply with Federal Rule of Civil Procedure 26(a)(2)(B), and none of them involved experienced cybersecurity experts. *Andrews* v. *Woody*, 2018 WL 2452177, at *4 (E.D. Va. May 31, 2018) (three paragraphs devoted to opinion); *Georges* v. *Dominion Payroll Servs., LLC*, 2018 WL 2088751, at *4 (E.D. Va. May 4, 2018) (two paragraphs). Plaintiffs' other cases likewise miss the mark. *Robles* v. *United States*, 2020 WL 8254267 (E.D. Va. Oct. 15, 2020) involved an expert in a negligence case who opined that the conduct fell below the standard of care without actually identifying the appropriate standard of care. *Id.* at *3. The court's discussion of the expert's

experience came in the context of addressing the expert's failure to explain "how his experience provides the relevant standard of care." *Id.* In *Copeland*, a copyright infringement case, the court already had doubts that plaintiffs' expert, who had never offered expert testimony before, was actually qualified. *Copeland* v. *Bieber*, 2016 WL 7079569, at *5–6 (E.D. Va. Sept. 8, 2016) ("the record before the court does not conclusively establish that Arnold is qualified as an expert by knowledge, skill, experience, training, or education regarding musical similarity"). The court ultimately excluded plaintiff's expert because he only offered "subjective" opinions where the law required analysis of objective criteria, and he provided no explanation "at all" about how his experience and technical expertise informed his opinions. *Id.* Notably, plaintiffs' expert also "expressly" disclaimed reliance on any specialized expertise he may have in forming his opinion. *Id.*

VI. MR. FERRANTE DID NOT RELY ON "FIELD TESTING" DONE FOR THIS CASE IN FORMING ANY OF HIS OPINIONS.

Plaintiffs' request to exclude Mr. Ferrante because he performed undisclosed "field testing" is baseless. While Mr. Ferrante, during the course of his deposition testimony, made references to signing on to websites—what he called "field tests"—to observe how data traversed the Internet in digital advertising transactions, he did not rely on these so-called "field tests" in forming his opinions. He performed these demonstrations to show his "younger staff" how information traversed the Internet. As he explained:

> Open bidding is a framework that uses secure communications. And what I did as an expert in the industry and know how communications work, whether it's clear text or encrypted communications, I through the course of my career, have conducted thousands of tests, man-in-the-middle tests, packet sniffing tests on encrypted communications, thousands, because that [is] what I do. I mean, that's my job. I did it for the government; I do it here in private practice.

> Once retained by Google and investigating header bidding versus open bidding of course we looked at the communications types; clear text versus encrypted. And so we demonstrated to ourselves like, look, here's the difference between the two. So all we needed [] was one in this particular case because it confirmed what we already knew. And if I'm being honest, we did it to the benefit of the younger staff.

Ferrante Dep. at 239:13–240:8. The "field test" simply confirmed what he "already knew" based on the thousands of prior tests he performed in the course of his work at the FBI and in private practice.

CONCLUSION

For the above reasons, the Court should deny Plaintiffs' motion to exclude Mr. Ferrante's testimony.

Dated: May 17, 2024

Respectfully submitted,

/s/ Craig C. Reilly

Craig C. Reilly (VSB # 20942)
THE LAW OFFICE OF
CRAIG C. REILLY, ESQ.
209 Madison Street, Suite 501
Alexandria, VA 22314
Telephone: (703) 549-5354
Facsimile: (703) 549-5355
craig.reilly@ccreillylaw.com

Karen L. Dunn (*pro hac vice*)
Jeannie S. Rhee (*pro hac vice*)
William A. Isaacson (*pro hac vice*)
Amy J. Mauser (*pro hac vice*)
Martha L. Goodman (*pro hac vice*)
Bryon P. Becker (VSB #93384)
Erica Spevack (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, NW
Washington, D.C. 20006-1047
Telephone: (202) 223-7300
Facsimile (202) 223-7420
kdunn@paulweiss.com

Meredith Dearborn (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
535 Mission Street, 24th Floor
San Francisco, CA 94105
Telephone: (628) 432-5100
Facsimile: (202) 330-5908
mdearborn@paulweiss.com

Erin J. Morgan (*pro hac vice*)
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
1285 Avenue of the Americas
New York, NY 10019-6064
Telephone: (212) 373-3387
Facsimile: (212) 492-0387
ejmorgan@paulweiss.com

Eric Mahr (*pro hac vice*)
Andrew Ewalt (*pro hac vice*)
Julie Elmer (*pro hac vice*)
Lauren Kaplin (*pro hac vice*)
Scott A. Eisman (*pro hac vice*)
Jeanette Bayoumi (*pro hac vice*)
Claire Leonard (*pro hac vice*)
Sara Salem (*pro hac vice*)
Tyler Garrett (VSB # 94759)
FRESHFIELDS BRUCKHAUS DERINGER US LLP
700 13th Street, NW, 10th Floor
Washington, D.C. 20005
Telephone: (202) 777-4500
Facsimile: (202) 777-4555
eric.mahr@freshfields.com

Daniel Bitton (*pro hac vice*)
AXINN, VELTROP & HARKRIDER LLP
55 2nd Street
San Francisco, CA 94105
Telephone: (415) 490-2000
Facsimile: (415) 490-2001
dbitton@axinn.com

Bradley Justus (VSB # 80533)
AXINN, VELTROP & HARKRIDER LLP
1901 L Street, NW
Washington, D.C. 20036
Telephone: (202) 912-4700
Facsimile: (202) 912-4701
bjustus@axinn.com

Counsel for Defendant Google LLC